2181
#2

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re the Application of	:	
Yoshihito Taninaka and Noriaki Ohura	:	Group Art Unit: 2181
Appl. No. 10/092,814	:	
Filed: 03/07/2002	:	
For: SECURITY LEVEL INFORMATION OFFERING METHOD AND SYSTEM	:	

Hon. Commissioner of Patents
and Trademarks
Washington, D.C. 20231

Certificate of Mailing Under 37 CFR §1.8(a)

I hereby certify that this correspondence is being deposited on 6/3/02 with the United States Postal Service as first class mail in an envelope properly addressed to COMMISSIONER OF PATENTS AND TRADEMARKS, Washington, D.C. 20231.

6/3/02
Date of Certificate

Cheryl M. Matticks
Cheryl M. Matticks

CLAIM FOR PRIORITY

In the inventors' Declaration filed March 7, 2002, the Applicants in the above-identified application claimed the benefit of priority under 35 U.S.C. §119 of their Japanese Application No. 2002-010888. Pursuant to §119 and 37 C.F.R. §1.55, we are filing herewith a certified copy of the Japanese Application No. 2002-010888 filed 01/18/2002.

Respectfully submitted,

DANN, DORFMAN, HERRELL AND SKILLMAN
A Professional Corporation
Attorneys for Applicant(s)

By _____
ROGER W. HERRELL, ESQ.
PTO Registration No. 22,964
1601 Market Street - Suite 720
Philadelphia, PA 19103-2307
Telephone: 215.563.4100
Facsimile: 215.563.4044

Enclosure: Priority document

日　本　国　特　許　庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

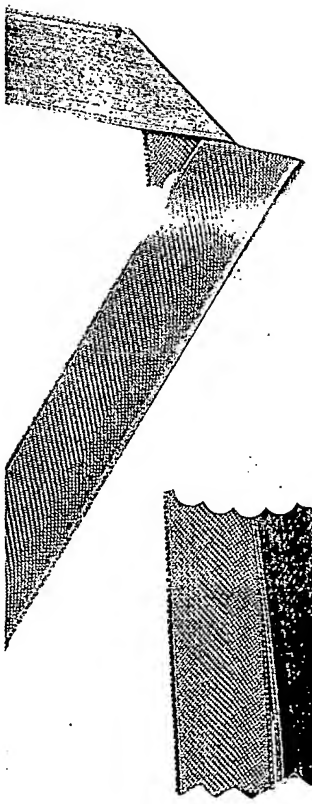
This is to certify that the annexed is a true copy of the following application as filed with this Office

出願年月日
Date of Application: ２００２年　１月１８日

出願番号
Application Number: 特願２００２－０１０８８８

[ST.10/C]: [ＪＰ２００２－０１０８８８]

出願人
Applicant(s): 株式会社チームガイア



CERTIFIED COPY OF
PRIORITY DOCUMENT

２００２年　３月１５日

特許庁長官
Commissioner,
Japan Patent Office

及川耕造

出証番号　出証特２００２－３０１７１０５

【書類名】　特許願
【整理番号】　Y02B002
【あて先】　特許庁長官　殿
【国際特許分類】　G06F 19/00
【発明者】
【住所又は居所】　東京都品川区上大崎３丁目１４番３７号　株式会社チームガイア内
【氏名】　谷中　義人
【発明者】
【住所又は居所】　東京都品川区上大崎３丁目１４番３７号　株式会社チームガイア内
【氏名】　大浦　則昭
【特許出願人】
【住所又は居所】　５０１００６８８２
【氏名又は名称】　株式会社チームガイア
【代理人】
【識別番号】　100104215
【弁理士】
【氏名又は名称】　大森　純一
【選任した代理人】
【識別番号】　100104411
【弁理士】
【氏名又は名称】　矢口　太郎
【手数料の表示】
【予納台帳番号】　069085
【納付金額】　21,000円
【提出物件の目録】
【物件名】　明細書　1
【物件名】　図面　1

【物件名】　　要約書　1

【プルーフの要否】　　要

【書類名】　明細書

【発明の名称】　セキュリティレベル情報提供方法及びシステム

【特許請求の範囲】

【請求項１】（ａ）　特定の機器の環境情報に基づいて、この機器についての脆弱点を特定し、この脆弱点の情報を前記機器に関連付ける工程であって、この脆弱点の情報は、この脆弱点の脅威レベル値を含み、

（ｂ）特定の機器について、この機器の種別、この機器について未だ対策を採っていない脆弱点の脅威レベル値、未対応の日数から当該機器の当該脆弱点に関するセキュリティレベル値を算出する工程と

（ｃ）前記（ｂ）工程で求めたセキュリティレベル値に基づいてセキュリティレベル情報を出力する工程と

を含むことを特徴とするセキュリティレベル情報提供方法。

【請求項２】　請求項１記載のセキュリティレベル情報提供方法において、

さらに、

（ｄ）当該機器に関連付けられた未対応の脆弱点が複数ある場合、各脆弱点に関するセキュリティ値を比較し、各脆弱点のセキュリティ値のうち最も脅威度の高いセキュリティ値を当該機器のセキュリティ値として算出する工程を有し、

前記（ｃ）工程は、当該機器のセキュリティ値に基づいてセキュリティレベル情報を出力するものである

ことを特徴とするセキュリティレベル情報提供方法。

【請求項３】　請求項２記載のセキュリティレベル情報提供方法において、

さらに、

（ｅ）ネットワークに接続された機器が複数ある場合、各機器に関するセキュリティ値を比較し、各機器のセキュリティ値のうち最も脅威度の高いセキュリティ値を当該ネットワークのセキュリティ値として算出する工程を有し、

前記（ｃ）工程は、当該ネットワークのセキュリティ値に基づいてセキュリティレベル情報を出力するものである

ことを特徴とするセキュリティレベル情報提供方法。

【請求項４】　請求項１記載のセキュリティレベル情報提供方法において、

前記（ｃ）工程は、

（ｂ）工程で求めたセキュリティ値と、機器やネットワークの基本構成等に基づいて算出した基本セキュリティ情報とに基づいてセキュリティ情報を出力するものである

ことを特徴とするセキュリティレベル情報提供方法。

【請求項５】　請求項１記載のセキュリティレベル情報提供方法において、

前記（ｃ）工程は、

当該システム若しくはこのシステムが接続されたネットワークのセキュリティ基準値との比較で前記セキュリティ値を表現する工程を含むものであることを特徴とするセキュリティレベル情報提供方法。

【請求項６】　コンピュータシステムのセキュリティレベルを算出するシステムであって、

監視対象のコンピュータシステムの環境情報を格納する環境情報格納部と、

更新された各種脆弱点情報であって少なくとも脆弱点の脅威レベル値を含む情報を格納する脆弱点情報格納部と、

前記環境情報に基づいて当該監視対象のコンピュータシステムに適用すべき脆弱点情報を前記脆弱点情報格納部から抽出し、このコンピュータシステムに関連付ける脆弱点情報提供部と

この脆弱点情報に基づいてシステムの管理者が修正作業を採ったかの情報を格納する脆弱点修正情報格納部と、

特定の機器について、この機器の種別、この機器について未だ対策を採っていない脆弱点の脅威レベル値、未対応の日数から当該機器の当該脆弱点に関するセキュリティレベル値を算出するセキュリティレベル算出部と、

前記算出部で求めたセキュリティレベル値に基づいてセキュリティレベル情報を生成し出力するセキュリティレベル情報生成部と

を有することを特徴とするセキュリティレベル情報提供システム。

【請求項７】　請求項６記載のセキュリティレベル情報提供システムにおいて

さらに、

当該機器に関連付けられた未対応の脆弱点が複数ある場合、各脆弱点に関するセキュリティ値を比較し、各脆弱点のセキュリティ値のうち最も脅威度の高いセキュリティ値を当該機器のセキュリティ値として算出するセキュリティレベル値比較部を有し、

前記セキュリティレベル情報生成部は、当該機器のセキュリティ値に基づいてセキュリティレベル情報を生成するものである

ことを特徴とするセキュリティレベル情報提供システム。

【請求項８】　請求項７記載のセキュリティレベル情報提供システムにおいて、

前記セキュリティレベル値比較部は、ネットワークに接続された機器が複数ある場合、各機器に関するセキュリティ値を比較し、各機器のセキュリティ値のうち最も脅威度の高いセキュリティ値を当該ネットワークのセキュリティ値として算出するものであり、

前記セキュリティレベル情報生成部は、当該ネットワークのセキュリティ値に基づいてセキュリティレベル情報を出力するものである

ことを特徴とするセキュリティレベル情報提供システム。

【請求項９】　請求項６記載のセキュリティレベル情報提供システムにおいて、

前記セキュリティレベル情報生成部は、

前記セキュリティレベル算出部で求めたセキュリティ値と、機器やネットワークの基本構成等に基づいて算出した基本セキュリティ情報とに基づいてセキュリティ情報を出力するものである

ことを特徴とするセキュリティレベル情報提供システム。

【請求項１０】　請求項６記載のセキュリティレベル情報提供システムにおいて、

前記セキュリティレベル情報生成部は、

当該システム若しくはこのシステムが接続されたネットワークのセキュリティ基準値との比較で前記セキュリティ値を表現するものであることを特徴とするセキュリティレベル情報提供システム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

この発明は、例えば、ネットワークに接続されたコンピュータシステム群のセキュリティレベルをリアルタイムで正確に評価し提供することができる方法及びシステムに関する。

【０００２】

【従来の技術】

最近、クラッカー等により企業や官公庁のネットワークやサーバが攻撃されたり、新種ウィルスに感染するという被害が多発している。このことにより、ネットワークセキュリティの強化に注目が集まっている。ネットワークセキュリティを強化するには、ネットワーク及びこのネットワークに接続された自社機器のセキュリティレベルを絶えず正確に把握しておく必要がある。

【０００３】

セキュリティレベルを評価するパラメータとしては、ネットワークやコンピュータのハードウエア及びソフトウエア的な構成といった静的な要素と、日々発生する脆弱点情報に応じて発生しそれに対応することによって変動する動的な要素とがある。企業活動にＩＴを利用する企業にとっては、この動的な要素に迅速に対応しなければ経営リスクが無限大に拡大することになるため、経営者にとってもその管理が非常に重要な課題となっている。

【０００４】

【発明が解決しようとする課題】

しかしながら、従来、このセキュリティレベルの把握はシステム管理者に任されており、経営者は、このシステム管理者からの報告を信じるしかなかった。一方、システム管理者の業務怠慢によりセキュリティレベルが低下等する場合もあり、このような要因を含めたセキュリティレベルの管理は非常に困難であった。

【０００５】

一方、経営者自身が、膨大なセキュリティ情報から自己のシステムに必要な情報を見つけ出して把握し、しかもその対策をタイムラグ無く施すことは専門技術

的に過ぎるため極めて困難である。

【０００６】

この発明は、このような事情に鑑みてなされたものであり、経営者等、セキュリティに関して十分な知識を有さない者であっても理解できるようなセキュリティ情報を、システム管理者の採った作業を反映して、迅速に提供できるシステム及び方法を提供することを目的とする。

【０００７】

【課題を解決するための手段】

上記課題を解決するため、この発明の第１の主要な観点によれば、（ａ）特定の機器の環境情報に基づいて、この機器についての脆弱点を特定し、この脆弱点の情報を前記機器に関連付ける工程であって、この脆弱点の情報は、この脆弱点の脅威レベル値を含み、（ｂ）特定の機器について、この機器の種別、この機器について未だ対策を採っていない脆弱点の脅威レベル値、未対応の日数から当該機器の当該脆弱点に関するセキュリティレベル値を算出する工程と、（ｃ）前記（ｂ）工程で求めたセキュリティレベル値に基づいてセキュリティレベル情報を出力する工程とを含むことを特徴とするセキュリティレベル情報提供方法が提供される。

【０００８】

このような構成によれば、未対応の脆弱点情報が存在する場合、機器の種別、その脆弱点の脅威レベル及び未対応の日数に基づいてセキュリティレベル値を算出し、それに基づいてセキュリティレベル情報を生成することができる。

【０００９】

また、この方法は、さらに、（ｄ）当該機器に関連付けられた未対応の脆弱点が複数ある場合、各脆弱点に関するセキュリティ値を比較し、各脆弱点のセキュリティ値のうち最も脅威度の高いセキュリティ値を当該機器のセキュリティ値として算出する工程を有し、前記（ｃ）工程は、当該機器のセキュリティ値に基づいてセキュリティレベル情報を出力するものであることが好ましい。

【００１０】

このような構成によれば、特定の機器に関連付けられた脆弱点情報が複数ある

場合、そのうちもっとも脅威度の高い脆弱点情報に基づくセキュリティ値を当該機器のセキュリティ値とすることができる。

【００１１】

この場合、さらに、（ｅ）ネットワークに接続された機器が複数ある場合、各機器に関するセキュリティ値を比較し、各機器のセキュリティ値のうち最も脅威度の高いセキュリティ値を当該ネットワークのセキュリティ値として算出する工程を有し、前記（ｃ）工程は、当該ネットワークのセキュリティ値に基づいてセキュリティレベル情報を出力するものであることが望ましい。

【００１２】

このような構成によれば、複数の機器がネットワークに接続されている場合、上述のようにして求めた各機器のセキュリティ値に基づいて、ネットワーク全体のセキュリティ値を算出することができる。

【００１３】

さらに、この発明の１の実施形態によれば、前記（ｃ）工程は、（ｂ）工程で求めたセキュリティ値と、機器やネットワークの基本構成等に基づいて算出した基本セキュリティ情報とに基づいてセキュリティ情報を出力するものである。

【００１４】

更なる別の１の実施形態によれば、前記（ｃ）工程は、当該システム若しくはこのシステムが接続されたネットワークのセキュリティ基準値との比較で前記セキュリティ値を表現する工程を含むものである。

【００１５】

このような構成によれば、当該システム若しくはネットワークが満たすべきセキュリティ値の基準値を定めておき、これとの比較で現在のセキュリティ値を表わすことができる。このことで、自社のセキュリティレベルの基準値を明確に把握していない経営者であっても、現在のセキュリティレベルが基準値との関係で相対的に表されるから容易に理解することができる。

【００１６】

また、この発明の第２の主要な観点によれば、コンピュータシステムのセキュリティレベルを算出するシステムであって、監視対象のコンピュータシステムの

環境情報を格納する環境情報格納部と、更新された各種脆弱点情報であって少なくとも脆弱点の脅威レベル値を含む情報を格納する脆弱点情報格納部と、前記環境情報に基づいて当該監視対象のコンピュータシステムに適用すべき脆弱点情報を前記脆弱点情報格納部から抽出し、このコンピュータシステムに関連付ける脆弱点情報提供部と、この脆弱点情報に基づいてシステムの管理者が修正作業を採ったかの情報を格納する脆弱点修正情報格納部と、特定の機器について、この機器の種別、この機器について未だ対策を採っていない脆弱点の脅威レベル値、未対応の日数から当該機器の当該脆弱点に関するセキュリティレベル値を算出するセキュリティレベル算出部と、前記算出部で求めたセキュリティレベル値に基づいてセキュリティレベル情報を生成し出力するセキュリティレベル情報生成部とを有することを特徴とするセキュリティレベル情報提供システムが提供される。

【００１７】

このような構成によれば、前記この発明の第１の観点に係る方法を実施することができるシステムが提供される。

【００１８】

なお、このシステムはさらに、当該機器に関連付けられた未対応の脆弱点が複数ある場合、各脆弱点に関するセキュリティ値を比較し、各脆弱点のセキュリティ値のうち最も脅威度の高いセキュリティ値を当該機器のセキュリティ値として算出するセキュリティレベル値比較部を有し、前記セキュリティレベル情報生成部は、当該機器のセキュリティ値に基づいてセキュリティレベル情報を生成するものであることが好ましい。この場合、前記セキュリティレベル値比較部は、ネットワークに接続された機器が複数ある場合、各機器に関するセキュリティ値を比較し、各機器のセキュリティ値のうち最も脅威度の高いセキュリティ値を当該ネットワークのセキュリティ値として算出するものであり、前記セキュリティレベル情報生成部は、当該ネットワークのセキュリティ値に基づいてセキュリティレベル情報を出力するものであることが望ましい。

【００１９】

また、この発明の他の1の実施形態によれば、前記セキュリティレベル情報生成部は、前記セキュリティレベル算出部で求めたセキュリティ値と、機器やネッ

トワークの基本構成等に基づいて算出した基本セキュリティ情報とに基づいてセキュリティ情報を出力するものである。

【００２０】

さらに、この発明の他の１の実施形態によれば、前記セキュリティレベル情報生成部は、当該システム若しくはこのシステムが接続されたネットワークのセキュリティ基準値との比較で前記セキュリティ値を表現するものであることが望ましい。

【００２１】

なお、この発明の他の特徴と顕著な効果は次の発明の実施形態の項及び添付した図面を参照することによって、より明確に理解される。

【００２２】

【発明の実施の形態】

以下、本発明の実施の形態を図面に基づき説明する。

【００２３】

図１中１で示すのがこの実施形態に係るセキュリティレベル情報提供システムであり、図1はこのシステム1の概略構成図である。

【００２４】

このシステム１は、ユーザＡ及びこのユーザＡの監視対象コンピュータシステム６に関する各種情報７～１１を格納するユーザシステムＤＢ２と、コンピュータシステム６の脆弱点に関する情報２４を格納する脆弱点ＤＢ３と、前記ユーザシステムＤＢ２に格納された各種ユーザ情報７～１１に基づいて前記脆弱点ＤＢ３内の脆弱点情報２４をユーザＡ側に提供すると共にそのセキュリティレベルを算出する脆弱点監視処理部４と、前記脆弱点情報２４を生成し前記脆弱点ＤＢ３を更新する脆弱点ＤＢ更新部５とからなる。

【００２５】

ユーザシステムＤＢ２には、ユーザ毎に、前記コンピュータシステム６の環境情報７と、システム管理者情報８と、組織情報９と、脆弱点修正情報１０と、セキュリティレベル値１１とが格納される。

【００２６】

コンピュータシステム環境情報７としては、図２に示すように、コンピュータシステム名、管理者、設置場所、用途等の属性情報１２の他、ＣＰＵ種別やメモリ容量等のハードウエア構成１３、ＯＳ名やアプリケーションプログラム名等のソフトウエア構成１４、起動サービス等の設定１５、利用ネットワーク技術１６、ＵＰＳ等の関連機器１７、Ｒａｉｄ等のミラーリング１８、ファイヤーウォールやＩＤＳ名等のセキュリティ対策情報１９等が格納される。

【００２７】

図１に示すシステム管理者情報８には、監視対象システム６の管理者（図１に２１で示す）の氏名、その情報提供先アドレスが格納される。組織情報９には、前記管理者２１が属する組織の名称及びその組織の管理者（経営者；図に２２で示す）の氏名及び情報提供先アドレスが、前記システム管理者情報８に関連付けて格納される。

【００２８】

脆弱点修正情報１０は、前記システム管理者２１が脆弱点情報に基づいて施した脆弱点修正作業のログが、システム毎に記録されてなるものである。前記セキュリティレベル値１１は、図３に示すように、セキュリティ基準値１１ａと、セキュリティレベル値履歴１１ｂと、内的要因ポイント１１ｃからなる。セキュリティ基準値１１ａは、組織の経営者（組織管理者２２）に対してその組織のセキュリティレベルを示すための基準値であり、予め当該組織でセキュリティに関する事故が発生した場合の損害や株価の影響などを考慮して決定され格納される。また、セキュリティレベル値履歴１１ｂには、過去に算出したセキュリティレベルが履歴として格納される。内的要因ポイント１１ｃは、後で詳しく説明するようにセキュリティレベル値を求めるために用いるものである。

【００２９】

一方、脆弱点ＤＢ３には、脆弱点情報４として、図４に示すように、脆弱点の概要情報を含む脆弱点概要情報２５と、当該脆弱点による脅威について記述した脅威情報２６と、当該脆弱点を修正するための脆弱点パッチ情報２７と、前記修正を実際のシステムで検証した結果を記述する脆弱点検証情報２８と、各脆弱点情報の脅威に関して重み付けをするための脅威レベル値２９が格納されている。

これらの情報の生成は、図５に示すように、このシステム１の運営者が、まず、外部ベンダーから主に英語で提供された脆弱点情報やパッチ情報を収集、翻訳し（ステップＳ１）、技術的な検証をする（ステップＳ２）。そして、各脆弱点情報に独自の脅威レベル値２９を付し（ステップＳ３）、前記脆弱点ＤＢ３を更新する（ステップＳ４）。このＤＢ３の更新は、前記ＤＢ更新部５を通して行う。

【００３０】

一方、前記脆弱点監視処理部４は、図１に示すように、このシステム１にアクセスするユーザの認証を行うユーザ認証部３０と、システム管理者２１等から環境情報７及び管理者情報８の入力を受け付けてこれらを更新する環境情報／管理者情報／組織情報登録部３１と、前記脆弱点ＤＢ３から脆弱点情報２４を取り出して前記システム管理者２１に提供する脆弱点情報提供部３２と、システム管理者２１からこのシステム管理者２１が前記脆弱点情報２４に基づいて施した修正作業記録の入力を受取り前記脆弱点修正情報１０として記録する脆弱点修正作業ログ記録部３３と、この修正情報１０に基づいて脆弱点対策情報を生成し、前記組織の管理者（経営者２２）にレポートする脆弱点対策情報作成部３４と、前記脆弱点情報２４とこれに対する修正情報１０に基づいて当該組織のセキュリティレベルを算出するセキュリティレベル算出部３５と、算出したセキュリティレベルに基づく情報を前記組織管理者（経営者２２）に提供するセキュリティレベル情報作成部３６とを有する。

【００３１】

これらの構成要素は、実際には、一般的なコンピュータシステムに設けられたハードディスク等の記憶媒体にインストールされた１又は２以上のコンピュータソフトウエアプログラムによって実現され、このコンピュータソフトウエアプログラムは前記コンピュータシステムのＣＰＵによってＲＡＭ上に呼び出され適宜実行されることでこの発明の機能を奏するようになっている。

【００３２】

以下、上記構成要素の構成及び機能の詳しい説明を、図６以下の画面構成図に基づき、実際の動作を参照して説明する。

【００３３】

図６は、このシステム１へのログイン画面の例である。

【００３４】

例えば、前記システム管理者２１が前記システム１に接続する場合、自己の端末からインターネット等を通して接続し、このログイン画面を立上げる。そして、このログイン画面のユーザ名入力ボックス４０およびパスワード入力ボックス４１にそれぞれ必要な情報を入力し、「Ｇｏ」ボタン４２を押す。このことで、前記ユーザ認証部３０が当該システム管理者２１の認証を行い、この監視システム１への接続を確立する。

【００３５】

接続者がシステム管理者２１である場合、前記脆弱点情報提供部３２が前記の認証結果に従い、図７に示す画面を前記システム管理者２１の端末上に表示させる。この画面には、修正ソフトウエアの適用を推奨するコンピュータ群４４が表示されている。このような表示を行わせるためには、前記監視対象コンピュータシステム６の環境情報７が前記ユーザシステムＤＢ２に適切に登録されている必要がある。この環境情報の入力及び更新を行うには、この図７の画面の環境登録ボタン４５を押す。

【００３６】

このボタン４５が押されると、前記環境情報／管理者情報／組織情報登録部３１が、図８に示す画面を表示する。システム管理者２１はこの画面を通してこの監視対象のコンピュータシステムの環境情報を入力することができる。この実施例では、この画面のコンピュータリスト４６に示されるように、このシステム管理者２１の属する組織は、東京本社と名古屋工場とを有し、東京本社には監視対象としてＭＡ－Ｔ１、ＭＡ－Ｔ２、ＭＡ－Ｔ３の３台のコンピュータが、名古屋工場にはＭＡ－Ｎ１、ＭＡ－Ｎ２、ＭＡ－Ｎ３の３台のコンピュータがそれぞれ設けられネットワークに接続されている。

【００３７】

この画面に示すのは、このうちＭＡ－Ｔ１に関するシステム環境情報である。この画面を通し、図２で説明した各情報１２～１９を各システム毎に入力していく。ここで、システム管理者の登録は必須であり、このシステム管理者情報の編

集はこの図に４７で示す管理者登録ボタンを押すことによって行えるようになっている。

【００３８】

また、この実施形態においては、この画面に、自動診断ボタン４８が設けられており、この自動診断ボタン４８を押すことで、前記した各情報を自動的に監視対象コンピュータシステム６から取得することができるようになっている。すなわち、図１に示すように、前記コンピュータシステム６には、このコンピュータシステム６の環境情報を取得する環境情報取得システム６０が接続されている。そして、前記ボタン４８が押されることで、前記前記環境情報／管理者情報／組織情報登録部３１が前記環境情報取得システム６０を起動して前記コンピュータシステム６の環境情報の全て若しくは一部を取得させることができるようになっている。

【００３９】

脆弱点情報提供部３２は、システム管理者２１がこの脆弱点監視システム１にアクセスして来たならば、上記のようにして登録されたユーザシステムＤＢ２内の環境情報７と前記脆弱点ＤＢ３内の脆弱点情報２４とのマッチングを行う。そして、この脆弱点ＤＢ３内に前記システム６のハードウエア構成等に適合する脆弱点情報２４があったならば、このコンピュータをセキュリティ対策の必要なコンピュータとしてピックアップして、図７に示す画面の符号４４で示す一覧に表示する。この例では、前記した全てのコンピュータが、脆弱点修正の必要なコンピュータシステムとしてピックアップされている。このことで、各脆弱点情報２４が各監視対象のコンピュータシステムに関連付けられることになる。

【００４０】

システム管理者２１は、この画面から、脆弱点一覧ボタン４９を押すことで図９に示すように脆弱点一覧５０を閲覧することができる。この脆弱点の一覧表示は、前記属性情報１２に基づき、システム種別を基準として表示することもできるし、ＯＳを基準として表示することもできるし、ロケーションを基準として表示することもできる。そして、この画面から各脆弱点をクリックすることで、さらに詳細な情報にアクセスすることができる。この場合、前記脆弱点情報提供部

３２は、前記脆弱点ＤＢ３から図３に示す２５～２８の各詳細情報を取り出し、図１０に示すように表示する。

【００４１】

このことでこのシステム管理者２１はこの脆弱点の詳細を確認し、対策の要否を検討することが可能になる。この脆弱点を確認した後、この対策を採った場合には、この画面の作業ログボタン５１を押すことで、脆弱点修正作業の記録の入力を行う。

【００４２】

図１１は、この作業ログの入力画面である。この画面には、選択に係る脆弱点の修正に必要な作業が時系列的に列挙されており、システム管理者２１は、各必要な作業を採ったかを確認し、実施日を入力していく。

【００４３】

このように入力された脆弱点修正作業は、前記脆弱点修正作業ログ記録部３３によって前記ユーザシステムＤＢ２内に前記脆弱点修正情報１０として格納される。そして、図１１に列挙された全ての作業が終了した場合には、この対応が済んだものとして記録されることになる。なお、この画面には、「対象外」ボタン５２と、「暫定措置」ボタン５３が設けられている。前記脆弱点情報が当該システムに対応しないものであるときには、この対象外ボタン５２を押すことで処理済みとすることができる。また、暫定措置ボタン５３は、脆弱点に対応する有効なパッチが提供されておらず、後で対応する場合等に使用する。

【００４４】

次に、前記組織管理者２２がこの脆弱点監視システム１に接続する場合について説明する。

【００４５】

前記組織管理者２２がこのシステムにログインした場合、前記ユーザ認証部３０は、前記組織情報９に基づいて、組織管理者２２であることを検出する。このことに基づき、前記脆弱点情報提供部３２は、図１２に示すように、組織管理者２２向けに、脆弱点対策情報を生成して提示する。この脆弱点対策情報は、この画面に示されるように、例えば、管理者毎、システム毎に、脆弱点情報と、その

情報の発効日、対策を採った対応日を含む。対策をとった対応日は、前記修正情報１０から取得して表示されることになる。また、未だ対策をとっていない脆弱点に基づき、前記脆弱点ＤＢ３から、脅威情報２６等を取り出し、この画面に５４で示すように表示する。

【００４６】

このような画面により、組織管理者２２は、自己の組織に係るネットワーク若しくはこのネットワークに接続されたコンピュータシステムのセキュリティ管理状況を確認することが可能になる。また、このシステムは、システム管理者２１の採った修正作業を記録しておき、これを組織管理者２２に提示するようにしたから、この組織管理者２２は、システム管理者２１を適切に管理することができる。

【００４７】

また、図１２の画面から、改善状況の表示ボタン５５を押すと、前記セキュリティレベル算出部３５が起動し、各脆弱点毎のセキュリティレベルを算出する。また、このセキュリティレベル算出部３５は、脆弱点間、コンピュータ間のセキュリティレベル値を比較してコンピュータ毎及びネットワーク毎のセキュリティレベル値を算出するためのセキュリティレベル値比較部５９を有する。

【００４８】

図１３に示すように、前記セキュリティレベルは、第１のグラフ５６と第２のグラフ５７の２つのグラフで示される。

【００４９】

第１のグラフ５６は、修正プログラム適用率である。各脆弱点情報の発効日付別に、適用した修正プログラムの数が、棒グラフで示されている。このグラフは、発効日を基準とするから、先月発効した脆弱点情報は、当月に修正作業を行ったとしても、先月分としてカウントされる。

【００５０】

第２のグラフ５７は、前記修正結果に基づく、セキュリティレベルの変化を示す折れ線グラフである。以下、この第２のグラフ５７の表示手順について説明する。

【００５１】

まず、この実施形態では、セキュリティレベルは、「内的要因」、「外的要因」及び「その他」からなるものと定義される。

【００５２】

内的要因とは、セキュリティポリシーの有無や日々の運用状況、ネットワーク構成やセキュリティ機器の設置、設置状況等により評価される静的な値である。この内的要因は、例えば、３月若しくは半年に一回、セキュリティコンサルタントがチェックシートによって行った評価により導き出される。

【００５３】

外的要因とは、日々新たに発見される脆弱点情報により求められる動的な値である。この外的要因は、基本的に、脆弱点情報の対象となっている機器の種別、前記脆弱点情報中の脅威レベル値、この脆弱点情報が発効してから何日経過しているかの情報に基づいて、前記組織管理者がアクセスする毎に算出される。

【００５４】

セキュリティレベルの算入割合は、内的要因を７０パーセント、外的要因を２０パーセント、その他を１０パーセントとする。ただし、その他は、人為的なミス等を表しているので、この実施形態では評価対象外とする。したがって、この実施形態では、内的要因の最高値７０ポイント、外的要因の最高値２０ポイントの合計最高点９０ポイントとしてセキュリティレベル値を算出する。なお、前述したように、内的要因ポイントは、予め算出され、前記ユーザシステムＤＢ２内に格納されている。

【００５５】

図１４は、前記セキュリティレベル算出部３５によるセキュリティレベル値算出工程を示すフローチャートである。

【００５６】

この実施形態では、ネットワーク全体のセキュリティレベルを導き出すのに、まず、図１４のステップＳ５～Ｓ９で、このネットワークに属する複数のコンピュータ毎のセキュリティレベルを算出する。そして、ステップＳ１０～Ｓ１４で、このコンピュータ毎のセキュリティレベルを比較し最低のものをネットワーク

のセキュリティレベルとして採用する。

【００５７】

このため、前記セキュリティレベル算出部３５は、まず、ネットワークに属する複数のコンピュータのうちの１番目（ｎ＝１）のコンピュータの１番目の脆弱点情報から処理を開始する（ステップＳ５）。

【００５８】

そして、ユーザシステムＤＢ２から、当該コンピュータ（機器）の種別情報、前記脆弱点情報の脅威レベル値、この脆弱点情報が発行してから何日経過しているかの情報を取得し（ステップＳ６）、以下の式により、この脆弱点情報に関する外的要因ポイント値ｗｐｐを算出する（ステップＳ７）。

【００５９】

Ｗｐｐ＝２０＋ｈｐ×ｈｋ×ｉｌ×ｄａｔｅ

・ここでＷｐｐは、値が低いほど脅威が大きいことを意味する。

・ｈｐは、基準パラメータであり、ここではー１とする。

・ｈｋは、コンピュータ種別（機種種別）であり、セキュリティ機器については２点、その他の機器については１点とする。

・ｉｌは当該脆弱点情報に付加された前記脅威レベル値（図４の符号２９参照）であり、三段階に設定され、Ｓは４点、Ａは２点、Ｂは１点とされている。

・ｄａｔｅは、これまでに対応せずに経過した日数であり、前記脆弱点情報が発効した日と現在との差により求める。

【００６０】

この外的要因ポイント値ｗｐｐを、当該システムに適用された全ての未対応の脆弱点について求め（ステップＳ８）、その中で、最も値の小さいものを、当該コンピュータシステムの外的要因ポイント値ｗｐｐ（ｎ）として出力する（ステップＳ９）。

【００６１】

また、当該組織内のネットワークに属する全てのコンピュータシステムに対しても、同様に外的要因ポイント値ｗｐｐ（ｎ）を求めていく（ステップＳ１０）。このようにして、全てのコンピュータシステムについての処理が終了したなら

ば、ネットワーク中で最小のｗｐｐを、ネットワーク全体の外的要因ポイント値ｗｐｐ（ａｌｌ）とする（ステップＳ１１）。

【００６２】

ついで、前記セキュリティレベル算出部３５は、前記セキュリティレベル値１１から内的要因ポイント１１ｃを取得し（ステップＳ１２）、これに、前記外的要因ポイントｗｐｐ（ｎ）及びｗｐｐ（ａｌｌ）を加算することで、セキュリティレベル値（ＳＰ）を算出する（ステップＳ１３、Ｓ１４）。

【００６３】

次に、前記セキュリティレベル情報作成部３６が、セキュリティレベル値ＳＰと前記セキュリティ基準値１１ａ及びセキュリティレベル値履歴１１ｂを用いて図１３に示す第２のグラフ５７を作成する（ステップＳ１５）。

【００６４】

すなわち、この実施形態では、前記セキュリティレベル情報作成部３６は、前記セキュリティレベル値履歴１１ｂから、過去１年間の各月の末日のセキュリティレベル値を取り出し、それを各月のセキュリティレベル値とする。そして、現在求めたセキュリティレベル値ＳＰを当月のセキュリティレベル値とする。そして、これらのセキュリティレベル値を、図１３に示すように、前記セキュリティ基準値を中心値とする折れ線グラフ５７として表示する。

【００６５】

このような折れ線グラフによれば、専門知識の少ない経営者であっても、当該組織のセキュリティレベル値を一目で評価することが可能になる。

【００６６】

なお、この発明は、上記一実施形態に限定されるものではなく、発明の要旨を変更しない範囲で種々変形可能である。

【００６７】

例えば、上記一実施形態では、システム管理者及び組織管理者は、インターネット等を通して前記脆弱点監視システムから各種情報を受け取るようにしたが、これに限定されるものではない。例えば、Ｅ－ｍａｉｌ等の手段で各種情報を提供するようにしても良い。

【００６８】

また、前記セキュリティレベルの表示は、棒グラフ及び折れ線グラフで行うようにしたが、これに限定されるものではなく、具体的な数値を示すことで行なうようにしても良い。さらに、前記セキュリティレベルの具体的な算出方法は、この発明の要旨の範囲で種々変更可能である。例えば、内的要因ポイント利用せず、外的要因ポイントｗｐｐ、ｗｐｐ（ｎ）、ｗｐｐ（ａｌｌ）により求めたセキュリティレベルのみを提供するようにしても良い。

【００６９】

【発明の効果】

以上説明した構成によれば、セキュリティに関して十分な知識を有さない者であっても理解できるようなセキュリティ情報を簡便な構成で迅速に提供することができる。

【図面の簡単な説明】

【図１】

この発明の一実施形態を示す概略構成図。

【図２】

コンピュータシステム環境情報の構成を説明するための図。

【図３】

セキュリティレベル値の構成を説明するための図。

【図４】

脆弱点情報の構成を説明するための図。

【図５】

脆弱点ＤＢの更新工程を示す工程図。

【図６】

ログイン画面を示す図。

【図７】

システム管理者に対する情報提供画面を示す図。

【図８】

環境情報登録画面を示す図。

【図９】

脆弱点情報の一覧画面を示す図。

【図１０】

脆弱点情報の詳細画面を示す図。

【図１１】

脆弱点修正作業の入力画面を示す図。

【図１２】

組織管理者に対する情報提供画面を示す図。

【図１３】

組織管理者に対するセキュリティレベル情報の提供画面を示す図。

【図１４】

セキュリティレベル値の算出工程を示すフローチャート。

【符号の説明】

１…脆弱点監視システム

２…ユーザシステムＤＢ

３…脆弱点ＤＢ

４…脆弱点監視処理部

５…ＤＢ更新部

６…監視対象コンピュータシステム

７…コンピュータシステム環境情報

８…システム管理者情報

９…組織情報

１０…脆弱点修正情報

１１…セキュリティレベル値

１１ａ…セキュリティ基準値

１１ｂ…セキュリティレベル値履歴

１１ｃ…内的要因ポイント

１２…属性情報

１３…ハードウエア構成

１４…ソフトウエア構成

１５…設定

１６…利用ネットワーク技術

１７…関連機器

１８…ミラーリング

１９…セキュリティ対策情報

２１…システム管理者

２２…組織管理者

２４…脆弱点情報

２５…脆弱点概要情報

２６…脅威情報

２７…脆弱点パッチ情報

２８…脆弱点検証情報

２９…脅威レベル値

３０…ユーザ認証部

３１…環境情報／管理者情報／組織情報登録部

３２…脆弱点情報提供部

３３…脆弱点修正作業ログ記録部

３４…脆弱点対策情報作成部

３５…セキュリティレベル算出部

３６…セキュリティレベル情報作成部

５６…第１のグラフ

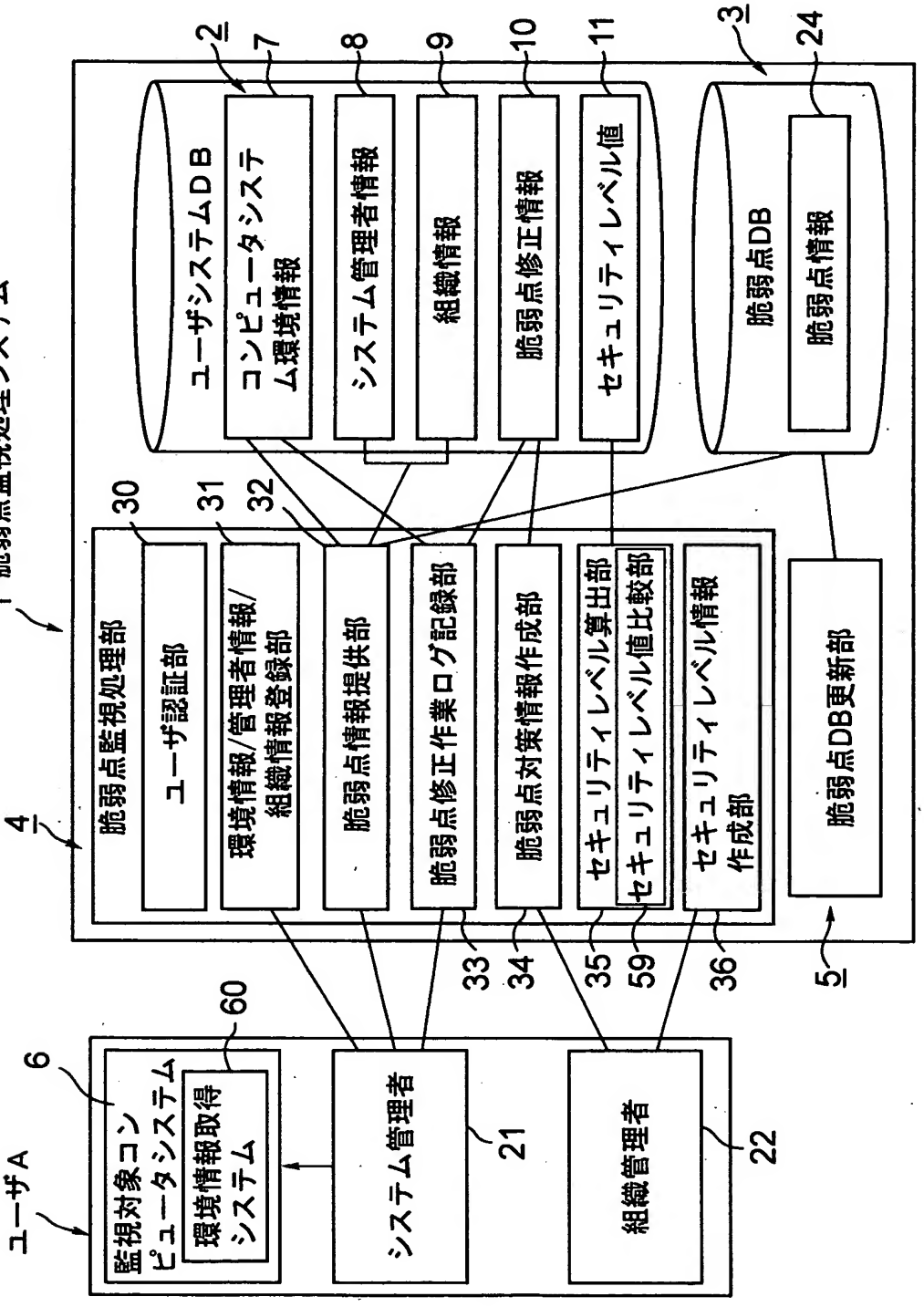
５７…第２のグラフ

５９…セキュリティレベル値比較部

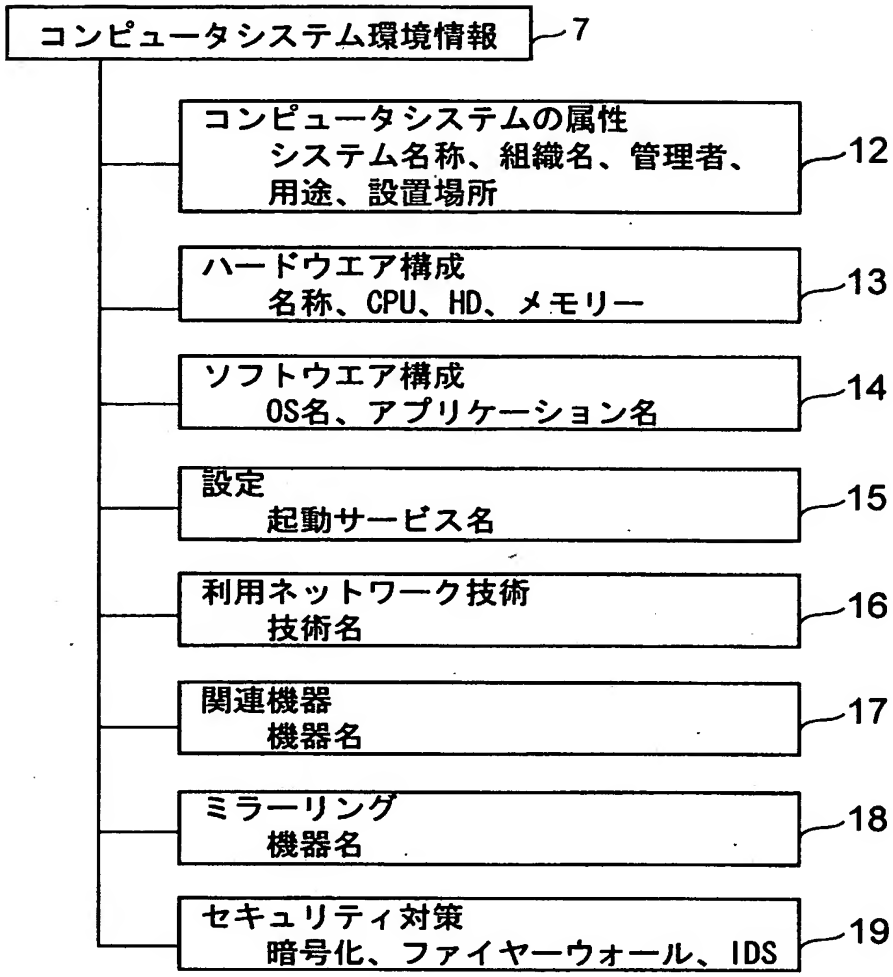
６０…環境情報取得システム

【書類名】　図面

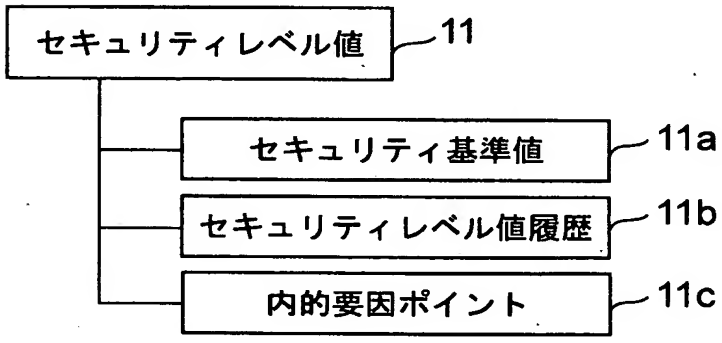
【図１】


1 脆弱点監視処理システム
2
7
8
9
10
11
3
24
ユーザシステムDB
コンピュータシステム環境情報
システム管理者情報
組織情報
脆弱点修正情報
セキュリティレベル値
脆弱点DB
脆弱点情報
4
30
31
32
脆弱点監視処理部
ユーザ認証部
環境情報/管理者情報/組織情報登録部
脆弱点情報提供部
脆弱点修正作業ログ記録部
脆弱点対策情報作成部
セキュリティレベル算出部
セキュリティレベル値比較部
セキュリティレベル情報作成部
脆弱点DB更新部
33
34
35
59
36
5
60
6
監視対象コンピュータシステム
環境情報取得システム
システム管理者
21
組織管理者
22
ユーザA

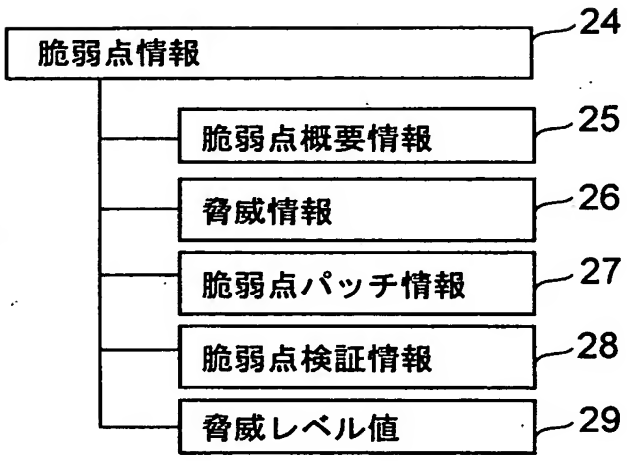
【図２】


コンピュータシステム環境情報
7
コンピュータシステムの属性
システム名称、組織名、管理者、
用途、設置場所
12
ハードウエア構成
名称、CPU、HD、メモリー
13
ソフトウエア構成
OS名、アプリケーション名
14
設定
起動サービス名
15
利用ネットワーク技術
技術名
16
関連機器
機器名
17
ミラーリング
機器名
18
セキュリティ対策
暗号化、ファイヤーウォール、IDS
19

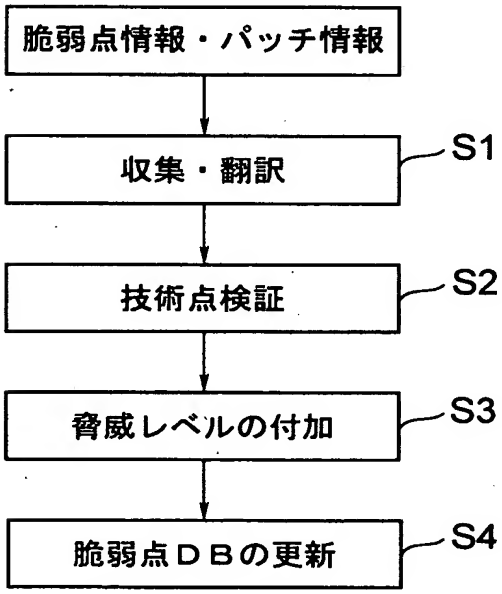
【図３】


セキュリティレベル値
11
セキュリティ基準値
11a
セキュリティレベル値履歴
11b
内的要因ポイント
11c

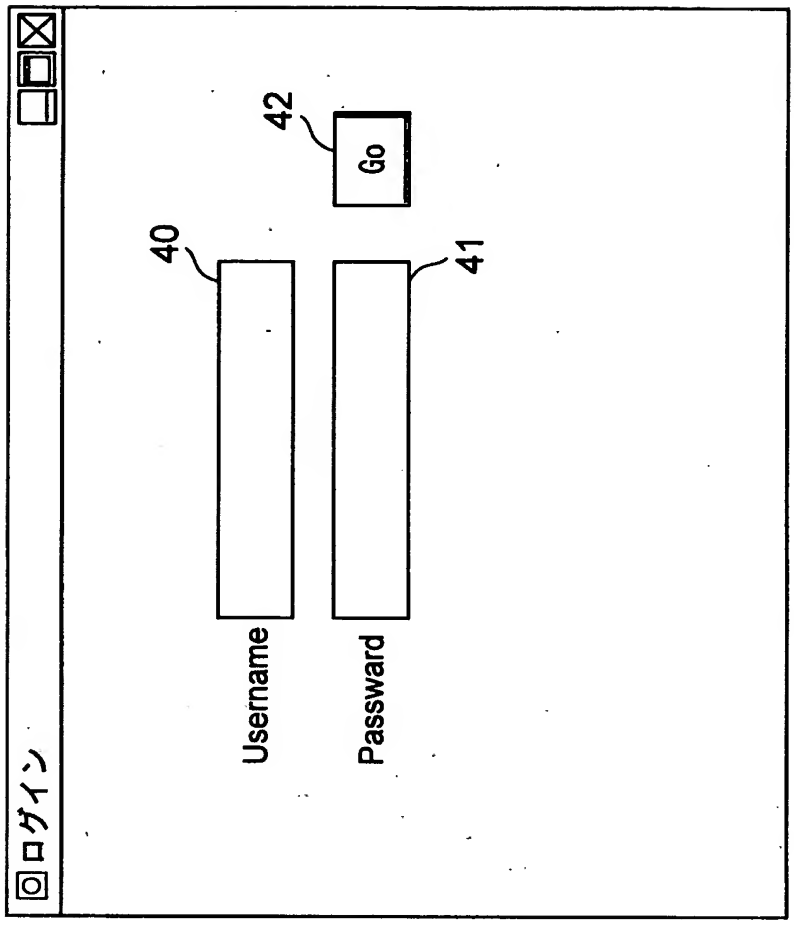
【図４】


脆弱点情報
24
脆弱点概要情報
25
脅威情報
26
脆弱点パッチ情報
27
脆弱点検証情報
28
脅威レベル値
29

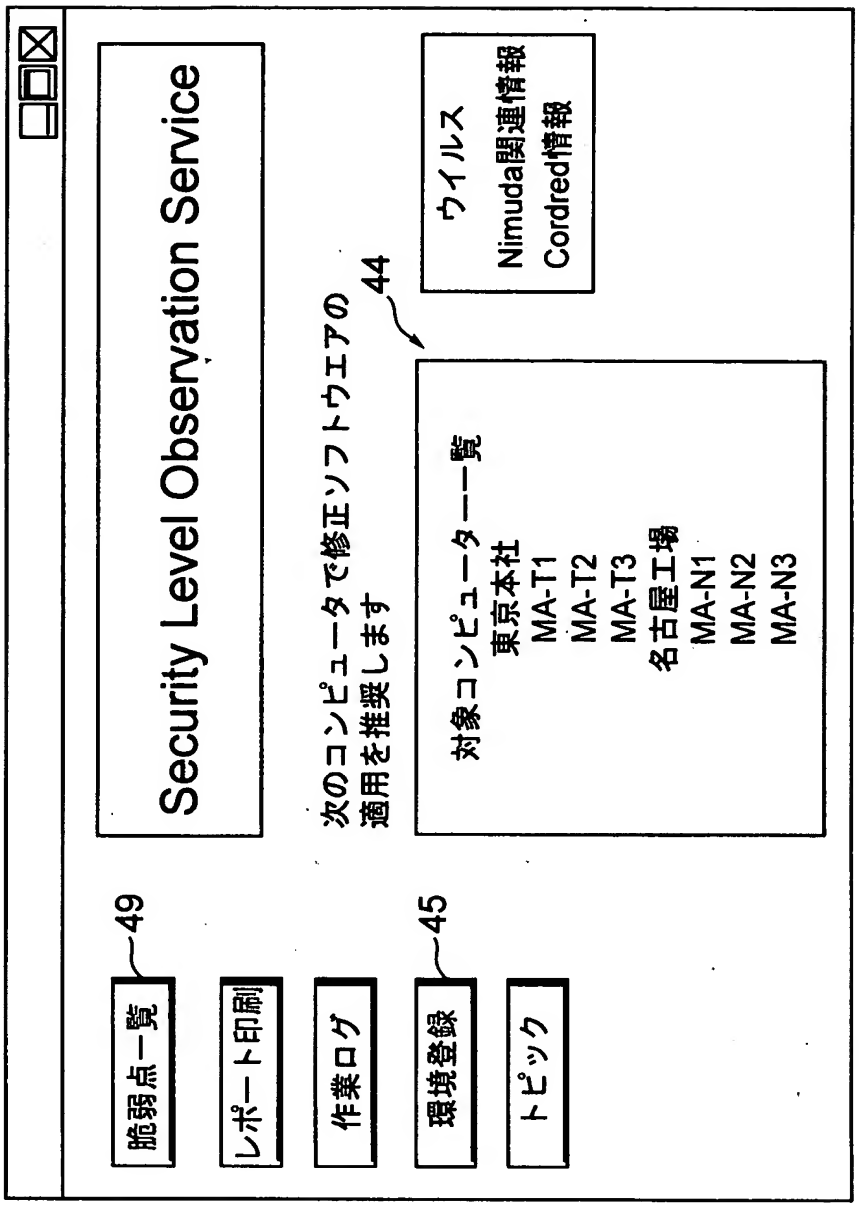
【図５】


脆弱点情報・パッチ情報
収集・翻訳
S1
技術点検証
S2
脅威レベルの付加
S3
脆弱点ＤＢの更新
S4

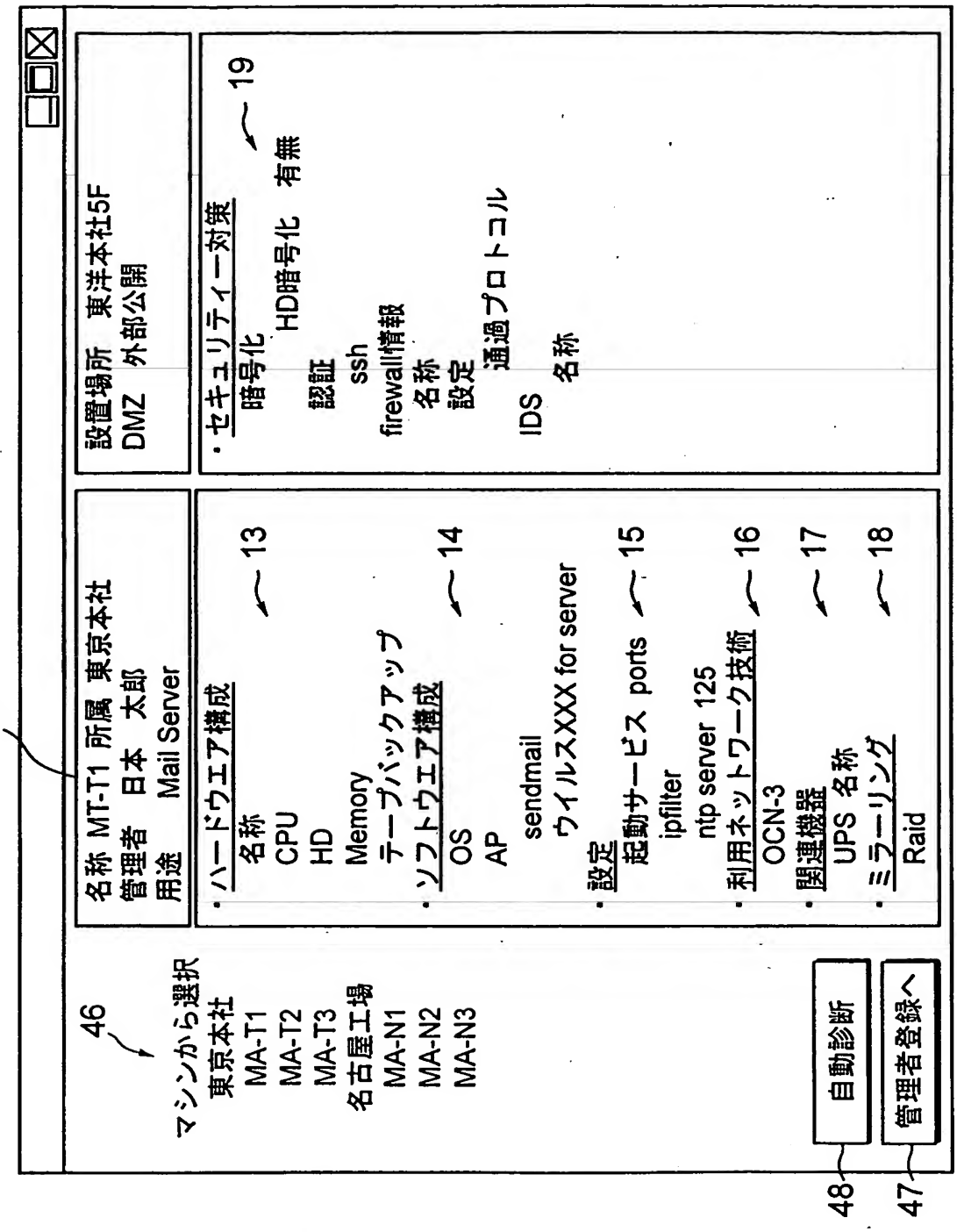
【図６】



【図７】


Security Level Observation Service
脆弱点一覧
49
レポート印刷
作業ログ
環境登録
45
トピック
次のコンピュータで修正ソフトウエアの
適用を推奨します
44
対象コンピューター一覧
東京本社
MA-T1
MA-T2
MA-T3
名古屋工場
MA-N1
MA-N2
MA-N3
ウイルス
Nimuda関連情報
Cordred情報

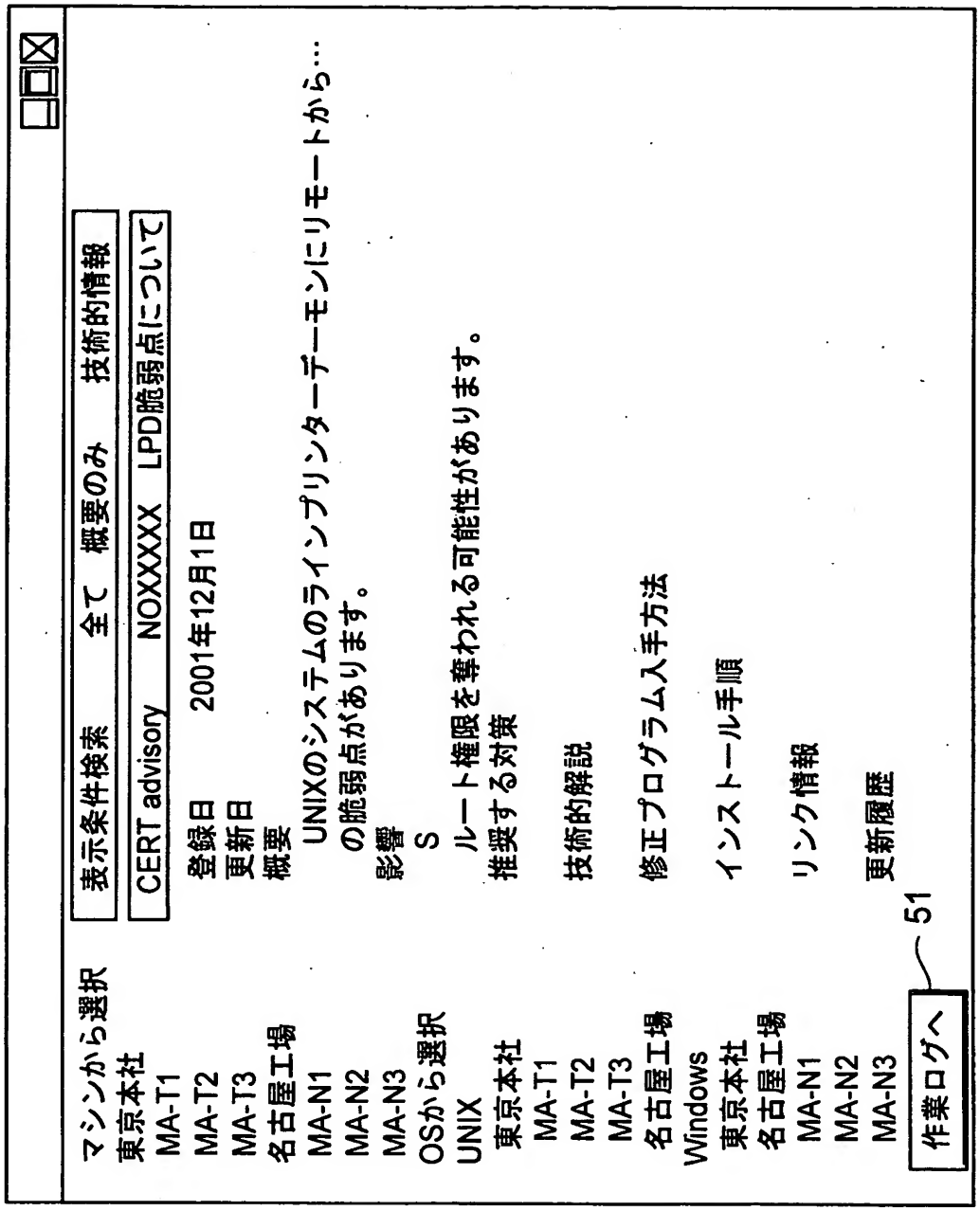
【図８】


12
46
マシンから選択
東京本社
MA-T1
MA-T2
MA-T3
名古屋工場
MA-N1
MA-N2
MA-N3
名称 MT-T1 所属 東京本社
管理者 日本 太郎
用途 Mail Server
・ハードウエア構成
名称
CPU
HD
Memory
テープバックアップ
13
・ソフトウエア構成
OS
AP
sendmail
ウイルスXXX for server
14
・設定
起動サービス ports
ipfilter
ntp server 125
15
・利用ネットワーク技術
OCN-3
16
・関連機器
UPS 名称
17
・ミラーリング
Raid
18
設置場所 東洋本社5F
DMZ 外部公開
・セキュリティー対策
暗号化
HD暗号化 有無
認証
ssh
firewall情報
名称
設定
通過プロトコル
IDS
名称
19
自動診断
48
管理者登録へ
47

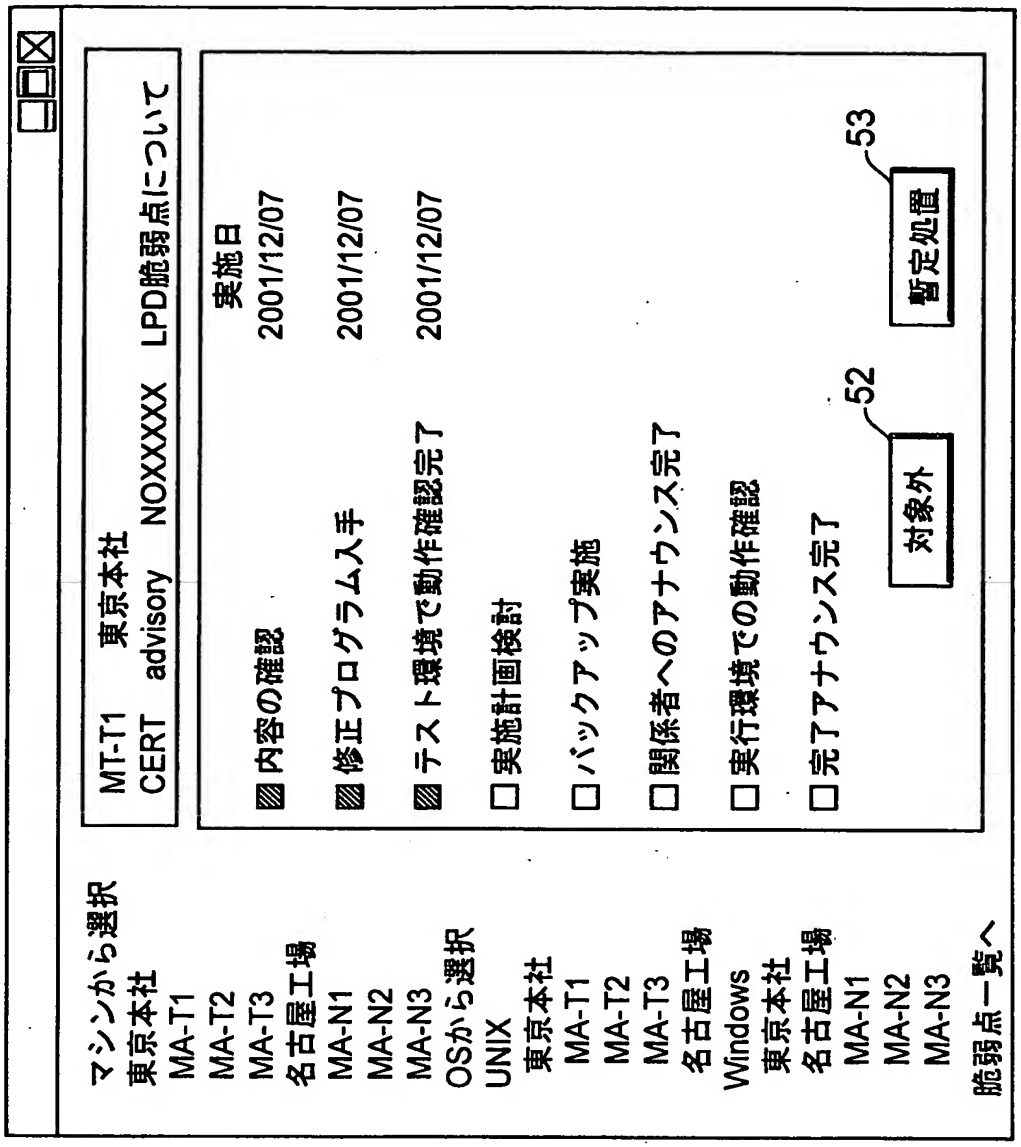
【図９】


50
マシンから選択
東京本社
MA-T1
MA-T2
MA-T3
名古屋工場
MA-N1
MA-N2
MA-N3
OSから選択
UNIX
東京本社
MA-T1
MA-T2
MA-T3
名古屋工場
Windows
東京本社
名古屋工場
MA-N1
MA-N2
MA-N3
条件検索　全て　未対応　対応済み　GO
MA-T1の脆弱点
CERT advisory　NOXXXXX　LPD脆弱点について
RSA advisory　NOXXXXX　ストリングフォーマットについて
CERT advisory　NOXXXXX　LPD脆弱点について
CERT advisory　NOXXXXX　LPD脆弱点について
MA-T2の脆弱点
CERT advisory　NOXXXXX　LPD脆弱点について
RSA advisory　NOXXXXX　ストリングフォーマットについて
CERT advisory　NOXXXXX　LPD脆弱点について
CERT advisory　NOXXXXX　LPD脆弱点について
マゼンダは未対応　青は対応

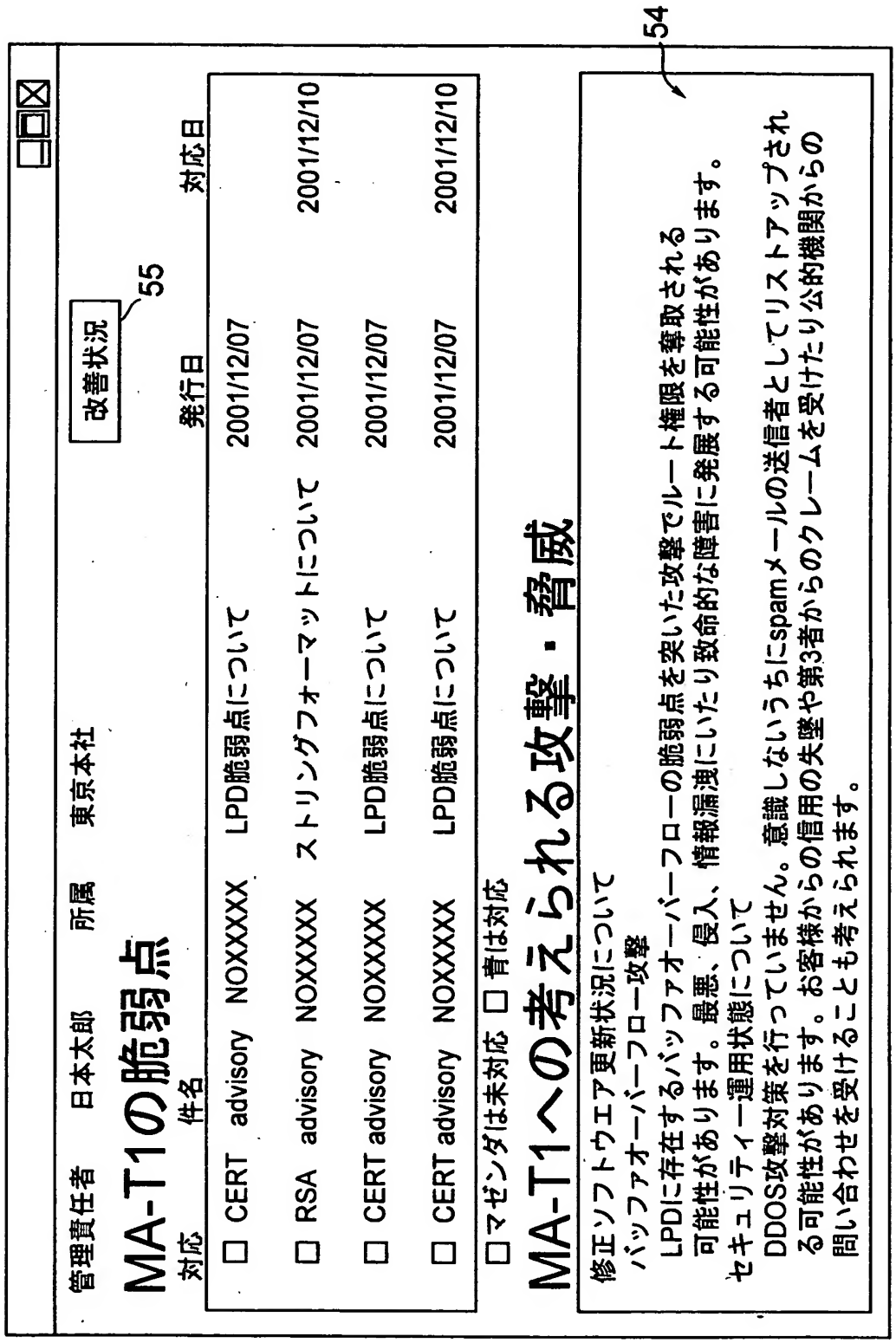
【図１０】


マシンから選択
東京本社
MA-T1
MA-T2
MA-T3
名古屋工場
MA-N1
MA-N2
MA-N3
OSから選択
UNIX
東京本社
MA-T1
MA-T2
MA-T3
名古屋工場
Windows
東京本社
名古屋工場
MA-N1
MA-N2
MA-N3
作業ログへ
51
表示条件検索　全て　概要のみ　技術的情報
CERT advisory　NOXXXXX　LPD脆弱点について
登録日　2001年12月1日
更新日
概要
UNIXのシステムのラインプリンターデーモンにリモートから…
の脆弱点があります。
影響
S
ルート権限を奪われる可能性があります。
推奨する対策
技術的解説
修正プログラム入手方法
インストール手順
リンク情報
更新履歴

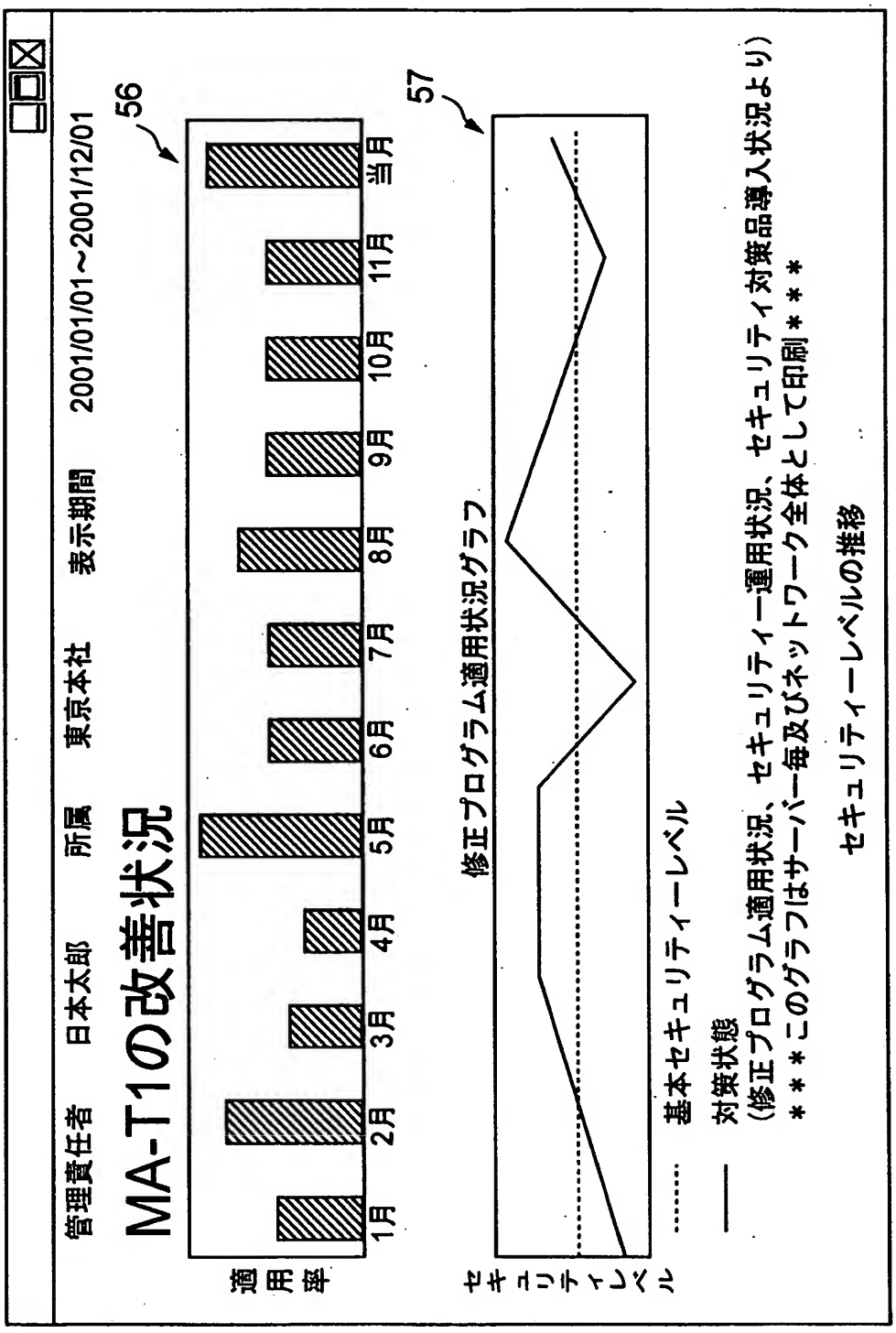
【図１１】


マシンから選択
東京本社
MA-T1
MA-T2
MA-T3
名古屋工場
MA-N1
MA-N2
MA-N3
OSから選択
UNIX
東京本社
MA-T1
MA-T2
MA-T3
名古屋工場
Windows
東京本社
名古屋工場
MA-N1
MA-N2
MA-N3
脆弱点一覧へ
MT-T1 東京本社
CERT advisory NOXXXXX LPD脆弱点について
実施日
内容の確認 2001/12/07
修正プログラム入手 2001/12/07
テスト環境で動作確認完了 2001/12/07
実施計画検討
バックアップ実施
関係者へのアナウンス完了
実行環境での動作確認
完了アナウンス完了
52
対象外
53
暫定処置

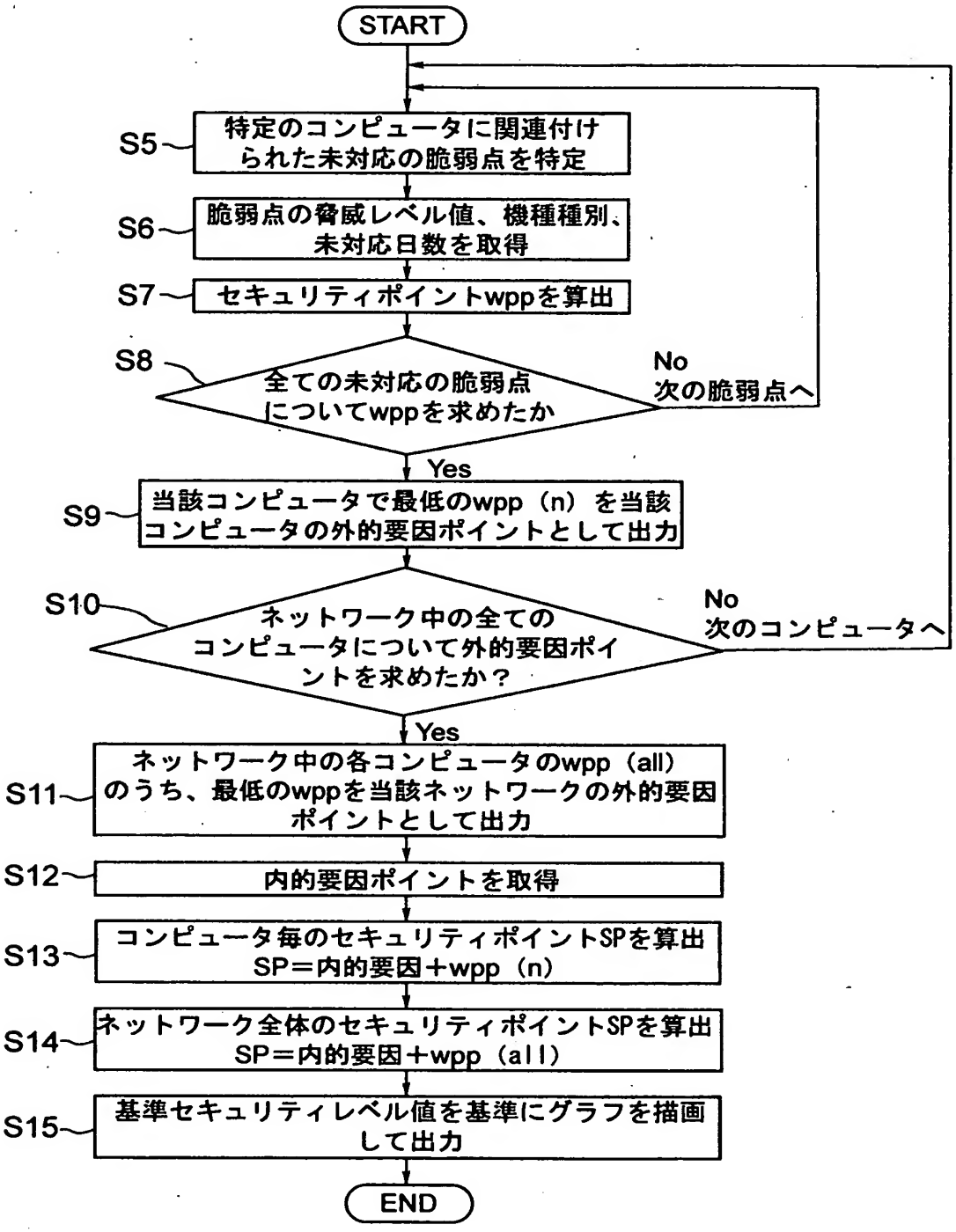
【図１２】


管理責任者　日本太郎　所属　東京本社
改善状況
55
MA-T1の脆弱点
対応　件名　発行日　対応日
□ CERT advisory NOXXXXX LPD脆弱点について 2001/12/07 2001/12/10
□ RSA advisory NOXXXXX ストリングフォーマットについて 2001/12/07 2001/12/10
□ CERT advisory NOXXXXX LPD脆弱点について 2001/12/07 2001/12/10
□ CERT advisory NOXXXXX LPD脆弱点について 2001/12/07 2001/12/10
□マゼンダは未対応 □青は対応
MA-T1への考えられる攻撃・脅威
54
修正ソフトウエア更新状況について
バッファオーバーフロー攻撃
LPDに存在するバッファオーバーフローの脆弱点を突いた攻撃でルート権限を奪取される可能性があります。最悪、侵入、情報漏洩にいたり致命的な障害に発展する可能性があります。
セキュリティー運用状態について
DDOS攻撃対策を行っていません。意識しないうちにspamメールの送信者としてリストアップされる可能性があります。お客様からの信用の失墜や第3者からのクレームを受けたり公的機関からの問い合わせを受けることも考えられます。

【図１３】


管理責任者　日本太郎　所属　東京本社　表示期間　2001/01/01～2001/12/01
MA-T1の改善状況
56
適用率
1月
2月
3月
4月
5月
6月
7月
8月
9月
10月
11月
当月
57
修正プログラム適用状況グラフ
セキュリティレベル
基本セキュリティーレベル
対策状態
(修正プログラム適用状況、セキュリティー運用状況、セキュリティ対策品導入状況より)
＊＊＊このグラフはサーバー毎及びネットワーク全体として印刷＊＊＊
セキュリティーレベルの推移

【図１４】


START
S5
特定のコンピュータに関連付けられた未対応の脆弱点を特定
S6
脆弱点の脅威レベル値、機種種別、未対応日数を取得
S7
セキュリティポイントwppを算出
S8
全ての未対応の脆弱点についてwppを求めたか
No
次の脆弱点へ
Yes
S9
当該コンピュータで最低のwpp（n）を当該コンピュータの外的要因ポイントとして出力
S10
ネットワーク中の全てのコンピュータについて外的要因ポイントを求めたか？
No
次のコンピュータへ
Yes
S11
ネットワーク中の各コンピュータのwpp（all）のうち、最低のwppを当該ネットワークの外的要因ポイントとして出力
S12
内的要因ポイントを取得
S13
コンピュータ毎のセキュリティポイントSPを算出
SP＝内的要因＋wpp（n）
S14
ネットワーク全体のセキュリティポイントSPを算出
SP＝内的要因＋wpp（all）
S15
基準セキュリティレベル値を基準にグラフを描画して出力
END

【書類名】　　要約書

【要約】

【課題】　セキュリティ技術に関して十分な知識を有さない者であっても理解できるように処理されたセキュリティ情報を提供する。

【解決手段】　少なくとも脆弱点の脅威レベル値を含む情報を格納する脆弱点情報格納部と、監視対象コンピュータシステムの環境情報に基づいて当該コンピュータシステムに適用すべき脆弱点情報を前記脆弱点情報格納部から抽出し、このコンピュータシステムに関連付ける脆弱点情報提供部と、この脆弱点情報に基づいてシステムの管理者が修正作業を採ったかの情報を格納する脆弱点修正情報格納部と、特定の機器について、その種別、この機器について未だ対策を採っていない脆弱点の脅威レベル値、未対応日数から当該機器の当該脆弱点に関するセキュリティレベル値を算出するセキュリティレベル算出部とを有する。

【選択図】　　図１

認定・付加情報

特許出願の番号	特願２００２－０１０８８８
受付番号	５０２０００６５０５９
書類名	特許願
担当官	末武　実　　１９１２
作成日	平成１４年　２月　５日

＜認定情報・付加情報＞

【提出日】	平成14年 1月18日
【特許出願人】	
【識別番号】	501006882
【住所又は居所】	東京都品川区上大崎３丁目１４番３７号
【氏名又は名称】	株式会社チームガイア
【代理人】	申請人
【識別番号】	100104215
【住所又は居所】	東京都港区南青山２丁目１３番７号　マトリス４Ｆ　大森・矢口国際特許事務所
【氏名又は名称】	大森　純一
【選任した代理人】	
【識別番号】	100104411
【住所又は居所】	東京都港区南青山２丁目１３番７号　マトリス４Ｆ　大森・矢口国際特許事務所
【氏名又は名称】	矢口　太郎

次頁無

出　願　人　履　歴　情　報

識別番号　　〔５０１００６８８２〕

１．変更年月日　　２００１年１０月３０日
［変更理由］　住所変更
住　所　　東京都品川区上大崎３丁目１４番３７号
氏　名　　株式会社チームガイア